Enhancing Data Security in the Cloud with Double Encryption: Strengths, Weaknesses and Best Practices

M.Pravallika[1] Dr. P. Bhargavi[2]
[1]Research Scholar, Dept. of Computer Science, Sri Padmavati Mahila Visvavidyalayam, Tirupati
[2] Assistant Professor, Dept. of Computer Science, Sri Padmavati Mahila Visvavidyalayam, Tirupati

Article Received: 10 May 2025, Revised: 06 June 2025, Accepted: 15 June 2025

Abstract—As Cloud computing adoption increases rapidly due to the benefits of scalability, cost-saving and flexibility, ensuring data security at rest and in transit within a cloud has become a serious concern. Double encryption, a method involving two layers of encryption using separate keys, offers a resilient solution for enhancing data security. This article summarizes the concept of double encryption, elaborates on its application, highlights its strengths and weaknesses, and discusses best practices for safeguarding data with optimal security measures.

Index Terms—Cloud Computing, Data Security, Double encryption, Digital Storage

I. INTRODUCTION

In today's digital era, the rapid advancement of cloud computing has transformed businesses by enabling them to migrate their operations to the cloud, offering unprecedented scalability, flexibility, and cost-saving benefits. However, the increased reliance on cloud services has also intensified concerns about data security. Traditional encryption methods are no longer sufficient to protect sensitive information from sophisticated cyber threats [3]. As businesses grapple with safeguarding sensitive information in cloud environments, the demand for advanced encryption methods has surged. One such method gaining prominence is double encryption, which enhances data security by applying two layers of encryption with distinct keys, thus creating an additional barrier against unauthorized access. This article examines the mechanism of double encryption, explores its application, benefits, and potential drawbacks, and provides best practices for implementing it in a cloud environment.

A. Cloud Computing and its benefits and services

Cloud Computing

Cloud Computing is "a model for enabling data storage and access over the internet rather than storing the information on our own computers or hard drive or data centers or servers, and delivery of computing services like servers, storage, databases, networking, etc., over the cloud with on-demand delivery or pay-as-you-go-pricing" [29].

Benefits

Computing offers various benefits

Scalability

Easily scale up or down the resources over the cloud based upon demand, flexibility and economic scale [1],[3],[4].

Cost Efficiency

Pay only for the infrastructure or resources utilized [1],[4].

Accessibility

Accessing the data, application or information over the internet from anywhere and at any time [1].

Disaster Recovery

Data can be stored on multiple servers rather than on a single server, which aids in backing up the information during data loss due to emergencies, such as hardware malfunction, malicious threats, or even simple user error [4].

Services

Cloud Computing offers various services.

Infrastructure-as-a-Service (IaaS)

IaaS provides virtualized computing resources or infrastructure for rent over the internet. It offers services like servers, storage, virtual machines, etc [1],[3],[4],[5].

Platform-as-a-Service (PaaS)

PaaS provides a platform to build, develop and deploy the application on cloud infrastructure [1],[3],[4],[5].

Software-as-a-Service (SaaS)

SaaS delivers software applications over the internet on a subscription basis, eliminating the need to install or maintain them [1],[3],[4],[5].

B. Data Security and its importance with the best approaches in the Cloud

Cloud computing has transformed the world of digital storage. With the help of this technology, the data can be stored and managed through remote servers rather than a local data center. However, with this accessibility, securing data on the cloud is becoming more complex, and it’s crucial to ensure the security of the data in the cloud [2].

Data Security is about protecting data and other digital information assets from unauthorized access, security threats, insider threats, etc., over the cloud. Cloud data is often highly sensitive, making it a target for cybercriminals. These cybercriminals are going to use different methods to access the data. So, effective measures need to be taken to provide security to the data in the cloud [2],[6].

Encryption plays a role in enhancing data security by protecting information from unauthorized access [2],[6]. There are two different approaches for securely encrypting data in the cloud.

- Single-Layer Encryption
- Double-Layer Encryption

The first approach is single-layer encryption, where the data is encrypted using symmetric or asymmetric key encryption. However, the key can be managed by the client, the provider, or both in a shared responsibility model.

The Second and best approach is double-layer encryption, where the data is encrypted twice with two distinct encryption key sets. Here, one set is managed by the cloud provider and the other set by the client.

II. Double Encryption

Double encryption is one of the advanced techniques that adds another layer of security to data. It involves encrypting the data twice with two distinct encryption keys. Here, it ensures that if one encryption layer is breached, the second layer protects for unauthorized access. Because of this, dual data encryption with two distinct keys enhances the organization's barriers against unauthorized access, assures that sensitive information remains secure [8], [9].

A. Key Management

The Double Encryption Key Management process incorporates several stages for securely handling the cryptographic keys of two layers. The following provides a comprehensive overview of the process.

a. Key Generation

Identify the purpose of the key

Decide whether the generating key is for encryption, decryption, digital signature or signature verification.

Decide whether both layers use symmetric encryption, asymmetric encryption, or a mix of both.

Select the Algorithm

In case of symmetric encryption, choose an algorithm like AES

In case of asymmetric encryption, choose an algorithm like RSA.

Decide Key Length

For symmetric encryption, use 128,192 or 256 bits (AES-256).

For asymmetric encryption, use 2048 or 4096 bits (RSA-2048).

Use a Secure Random Number Generator (RNG)

Generate a random sequence of bits that should be equal to the chosen key length in the case of symmetric encryption.

Generate random prime numbers or an elliptic curve based on the algorithm in the case of asymmetric encryption.

Create the key

Generate a key directly using the RNG for symmetric encryption.

Use an algorithm-specific key generation method for asymmetric encryption.

Test the Key

Key strength to be verified with statistical tests to ensure the generated key is truly random and meets algorithmic requirements.

Storage of the key

When the time of the key storage, the key should be encrypted with the higher-level master key and stored in a Hardware Security Module (HSM), in the case of asymmetric encryption, private keys are stored securely.

Protect the Key

Restrict access to the key based on role-based permissions.

To access the keys, maintain multifactor authentication on the systems.

Maintain a life cycle for the key, including rotation (regular and eventual).

Backup the Key
Back up the key in multiple secure locations.
Ensure backups are encrypted and physically separated.

Destroy Unused Keys
When a key is no longer needed, securely delete it using cryptographic wiping.

b. Key Distribution

Secure Channel
Use Secure mechanisms like TLS, VPNS, or hardware-based encryption for transmitting keys between systems.

Access Control
By maintaining strict role-based access controls, only authorized users can access keys.

Key Wrapping
Encrypt the data key using a master key before transmitting it.

c. Key Storage

Hardware Security Module
Use tamper hardware devices to store and manage keys securely and prevent unauthorized access or physical theft.

Segregated Storage
Keys used for each encryption layer should be stored in different locations or systems.
Encrypted Storage
Keys should be stored in an encrypted format using robust encryption standards to add a layer of protection.

d. Key Usage
Scoped Access
To avoid the misuse of the key, maintain key limits for specific applications, systems, etc.

Auditing
In each occurrence of key usage, a log file is maintained to know where the key is used, who accessed it and why.

Minimal Exposure
The keys are loaded into memory only when required. After usage, it is to be erased securely.

e. Key Rotation
Periodic Updates
To reduce the risk associated with prolonged use of a key, update a key regularly.

Layer-Specific Rotation
There should be no overlap while rotating keys in each layer of encryption. It should be independent.

Backward Compatibility

Ensure smooth mitigation between old and new keys by implementing a robust key rotation process.

f. Key Backup and Recovery

Redundant Backups

Preserve encrypted replicas of all keys for backup and store them securely in distinct locations.

Access Controls

Minimize the number of systems or users accessing the backup keys.

Disaster Recovery

Ensure that the regular recovery process is tested to address key loss or corruption.

g. *Key Revocation and Expiration*

Revocation Protocols

Ensure well-defined procedures are in place to revoke the keys that are compromised or no longer needed.

Expiration Policies

Set a lifespan for each key to ensure they are not used beyond their time limit, thereby reducing the risk of misuse.

h.Key Deletion

Secure Erasure

Utilize different methods and tools to delete keys securely, ensuring they can't be stored.

Verification

Validate the deletion process to ensure that the keys are fully deleted or not.

B. Working of Double Encryption

Initial Encryption (First Layer)

Encryption Key1

The data is encrypted with encryption algorithm 1 (e.g., RSA, AES) using a specific encryption key (Key1) [9].

Output

The result of this process is ciphertext, generated with the original data.

Secondary Encryption (Second Layer)

Encryption Key2

The ciphertext achieved from the first layer is again encrypted with encryption algorithm2 (E.g., RSA, AES) using another encryption key (Key2) [9].

Output

The result of the second encryption is the ciphertext, generated with the ciphertext of the first layer.

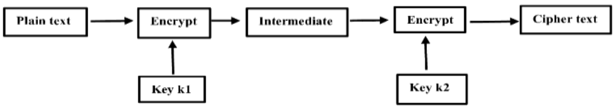

Figure 1. Double Encryption Process

Example

Let's take a simple example to understand the concept:

Step 1

Original or plain Text is encrypted with the AES algorithm using key1, generating Ciphertext 1.

Step 2

Ciphertext 1 is then encrypted again using the same AES or a different encryption algorithm with Key 2, generating Ciphertext 2. Ciphertext 2 is the final output of this double encryption technique, and can be stored or transmitted securely.

Decryption Process

The decryption Process is a complete reverse of the encryption process:

Initial Decryption

Key 2

Ciphertext2 is decrypted with the decryption algorithm by using key2, then it retrieves ciphertext 1.

Secondary Decryption

Key 1

Ciphertext 1 is decrypted with the decryption algorithm by using key 1, then it retrieves the original text.

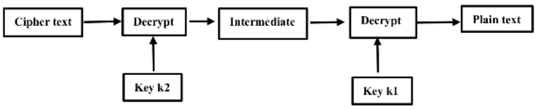

Figure 2: Double Decryption process

III. Benefits of Double Encryption

There are various advantages to implementing double encryption, such as enhancing security, flexibility and scalability, data integrity and confidentiality, compliance with regulatory requirements, increased customer trust, mitigation of insider threats, and risk mitigation, which makes a valuable investment for organizations.

Enhanced Security

Double encryption enhances data security by providing two layers of encryption. If one encryption layer is compromised, another layer secures the data and makes it complex for the attackers to access the data. This approach will provide a robust solution for protecting the data from unauthorized access [9].

Compliance with Regulatory Requirements

Most of the organizations don't meet the regulatory standards like GDPR, HIPAA and PCI-DSS, but they're satisfied with the double encryption method. These standards will provide a higher level of data security. It facilitates smoother audits and helps in obtaining necessary security certifications, demonstrating compliance and reducing the risk of legal penalties.

Data Integrity and Confidentiality

Double encryption reduces the risk of data breaches, assuring that sensitive information is maintained confidential and integrity, and organizations can securely share the data with partners or across different cloud environments, trusting that data is protected from unauthorized access because the data is encrypted twice.

Increased Customer Trust

Double encryption enhances customer trust by having a strong commitment towards data security through the double encryption.

Mitigation Of Insider Threats

With the help of the double encryption, the data is secured from inside threats by ensuring that even if employees have access to the encryption key cannot easily perform decryption on the data. Implementing more stringent and layered security policies makes it difficult for malicious insiders to compromise the data [9].

Flexibility and Scalability

Double encryption has the flexibility of adapting to security measures as needed, while implementing in various cloud environments like on-premises, hybrid, and multi-cloud setups. As organizations need to handle more data, double encryption can scale to meet increasing security demands without compromising performance.

Risk Mitigation

Double encryption reduces the overall risks of the information because of having two layers of encryption. If one of the encryption layers is compromised, another layer acts as an additional barrier to the data. It ensures the adoption of robust key management practices, and later it strengthens the overall security posture of the organizations [9].

IV. RELATED WORKS

This subsection describes the previous works on single-layer encryption and double-layer encryption using symmetric or asymmetric encryption, or a combination of both techniques. This review highlights several challenges it encounters when integrating these techniques in the context of double encryption.

Yash Bharadwaj and Shampa Chakraverty (2013) [16] have done research work on “A design Pattern for Symmetric encryption”. The authors propose a new Circular Design Pattern (CDP) that serves as a template for generating Dynamic Symmetric Encryption Frameworks (DSEF). This approach helps to reuse the existing algorithms to create new encryption strategies, enhancing security while maintaining reliability and rapid development capabilities. Here is a complexity for creating adaptable encryption techniques and systematic frameworks, and having potential challenges for ensuring compatibility between multiple encryption algorithms, managing performance overhead and maintaining security over cryptanalysis.

Mohammed Nasser Alenezi, Haneen Khalid Alabdulrazzaq and Nada Qasem Mohammad (2020) [17] have done research work on “Symmetric Encryption Algorithms: Review and Evaluation Study”. This Paper discussed the importance of data security and confidentiality when exchanging data over the internet, emphasizies the role of encryption and decryption

algorithms in protecting the data from unauthorized access while transmitting data over insecure channels by comparing the various symmetric encryption algorithms.
Here, it was found that these algorithms are not properly implemented in the double encryption method, which poses challenges of increased computational complexity that lead to decreased performance and higher CPU utilization and proper management of key distribution, because some algorithms may be susceptible to specific attacks.

K. Ragavan, Mohankumar B, K. Vivekrabinson, and R.A. Arun (2024) [18] have done research work on “A Double Layer Encryption for Communication using Cryptographic Algorithms”. This paper uses a double encryption method by combining the Vigenere and Polybius ciphers for enhancing communication security.
However, the common challenges identified here are performance overhead, complexity in implementation, User Accessibility, compatibility and risk of vulnerabilities.

Dahlan Abdullah, Robbi Rahim and Andysah Putera Utama (2018) [19] have done research work on “Super-Encryption Cryptography with IDEA and WAKE Algorithm”. This paper presents a combination of IDEA and WAKE algorithms to produce a secure ciphertext for protecting against cryptanalysts attacks and helps to enhance the overall security of the data.
However, the common challenges identified here are increased computational complexity that leads to slower performance, Vulnerability to advanced attacks, complicated tasks of key distribution and key storage and key management. These key management errors lead to compromised security.

L.S Abhiram, L. Gowrav, H.L. Punith Kumar, B.K. Sriroop, Manjunath C Lakkanavar (2014) [20] have done research work on “Design and synthesis of dual key based AES encryption”. This paper addresses dual dual-key-based AES encryption method that utilizes both a System key generated within the system and a user key provided by the user, and the proposed algorithm includes a new transformation called shift columns and is designed to be FPGA implementable, which ensures the security and efficiency in hardware applications. This paper also discusses the vulnerabilities of the AES encryption algorithm, particularly of static S-Boxes, which are susceptible to cryptanalysis attacks.
Here found that maintaining compatibility with existing systems and security against advanced cryptanalysis attacks are critical considerations, and also addresses the challenges of complexity in key management, Vulnerability of Static S- Boxes, and performance degradation because of additional encryption layers.

Zhuhong Shao, Yadong Tang, Mingxian Liang, Yuanyuan Shang, Wang Feng and Wang Yunfei (2020) [21] have done research work on “Double image encryption based on symmetry of 2D-DFT and equal modulus decomposition”. This paper presents a double image encryption scheme by utilizing the symmetry of the two-dimensional discrete Fourier transform (2D-DFT) and equal modulus decomposition (EMD) to enhance security. This method also embodies initial states from a 2D logistic map, which generates phase masks and rotation angles from plaintext images which enhancing security and effectiveness against Gaussian noise attacks.
However, the common challenges are key management complexities, maintaining a sufficient key length for security purposes, increased computational requirements leading to issues on performance and risk of vulnerabilities.

Taniya Hasija, K.R. Ramkumar, Bhupendra Singh, Amanpreet Kaur and S. Mittal (2023) [22] have done a research work on “Symmetric Key Cryptography: Review, Algorithmic Insights,

and Challenges in the Era of Quantum Computers". This paper presents the importance of security in this digital world, highlighting the role of cryptography in protecting sensitive information from unauthorized access and provides awareness to researchers and practitioners in cryptography for securing sensitive information from quantum attacks.
However, it addresses the challenges of computational complexity, performance issues, key management, key distribution and key storage.

D Chatterjee, J Nath, S Das, S Agarwal and A Nath (2012) [28] have done research work on "Symmetric Key Cryptography using modified DJSSA symmetric key algorithm". This paper presents a modified symmetric key cryptographic method known as the modified DJSSA algorithm that will enhance the process of encryption and decryption. So, this will increase security, making it difficult to access the actual key matrix with the help of brute force methods and supports parallel processing for the large files that will be handled by splitting into manageable parts for encryption and decryption.
Here it faces the challenges of computational complexity, slower performance for larger files and key management.

Swathi P and G. Sreeja Rajesh (2018) [23] have done research work on "Double Encryption using TEA and DNA". This paper proposed a new algorithm called DETD, which combines the TEA and DNA algorithms to increase the level of encryption for providing better security against intruders.
Here the challenges are taking a longer time for encryption and decryption, key management, increased computational complexity.

Akashdeep Bhardwaj, G.V.B. Subrahmanyam, Vinay Avasthi, and Hanumat G. Sastry (2015) [24] have done research work on "Security Algorithms for Cloud Computing Environment". This paper presents cryptography and its types, and it also addresses the vulnerabilities of the RSA Algorithm against mathematical attacks, which compromises security. To counter this vulnerability proposed new algorithm a new secure algorithm aimed at eliminating the distribution of the large number(n) that underpins the RSA algorithm's security.
However, it addresses the performance overhead, risk of key exposure and key management.
Anoushka Malhotra, Ashwin Arora and Dr. Manjot Kaur Bhatia (2022) [25] have done research work on "Symmetric Cryptographic Approaches". This paper presents the necessity of securing sensitive information in this digital world and compares various symmetric algorithms such as AES, DES,3DES, RC4 and Blowfish to provide a robust encryption and decryption process for secure communication against vulnerabilities.
However, it addresses the risk of vulnerabilities when two encryption processes are not adequately independent, secure handling of multiple keys becomes complicated, increased computational complexity leads to decreased performance and higher resource utilization.

Lei Ma, Mingfei Qu and Pengfei He (2022) [26] have done research work on "Double Encryption Algorithm for Massive Personal Biometric Authentication Images Based on Chaotic Mapping for Future Smart Cities". This paper presents a double encryption algorithm for personal biometric authentication with the method of bit scrambling and Secure Hash Algorithm (SHA)-256. It generates chaotic system initial values and an exclusive OR (XOR) operation that transforms chaotic sequences into ciphertext image matrices. This will result in increased encryption accuracy, efficiency and security performance.
Here, it addresses the challenges of securely managing key distribution, maintaining the algorithm's efficiency, speed and large key space against brute-force attacks, balancing encryption strength and computational performance is crucial.

Yifan Zhang, Chaoyu Yu, Yuqiang Wang, Junyu Han, Zhong Ming, Howard S. An and Ningping Yuan (2023) [27] have done a research work on "Application of Symmetric Key Algorithm in Data Security Design of Smart Grid". This paper focuses on applying symmetric key algorithms for enhancing data security in smart grids and validates this approach through experimental analysis by run-length test and frequency test methods to demonstrate the security and effectiveness of this context.
Here, it addresses the increased computational complexity, preventing vulnerabilities that need proper key management, and slower performance.

Bappaditya Jana, Jayanta Poray, Tamoghna Mandal and Mayal Kule (2017) [15] have done research work on "A Multilevel encryption technique in Cloud Security". This paper proposed multilevel encryption by using AES and the Round-shifted algorithm for enhancing security more than single-level encryption.
However, it addresses vulnerabilities in cloud security against intelligent intruders and key transmission threats.

Rima Akterm, Md. Ashikur Rahman Khan, Fuad Rahman, Sultana Jahan Soheli and Nusrat Jahan Suha (2023) [14] have done research work on " RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing". This paper proposed a hybrid encryption method using AES and RSA that enhances a data security.
Here, it addresses the scalability issues, improved authentication and access control mechanisms.

Soorya Kumar S, Meenakshi P and A Subramanyan (2022) [13] have done research work on "HASHING & DOUBLE ENCRYPTION TECHNIQUE FOR INFORMATION STORAGE IN CLOUD". This paper proposed a hybrid encryption system that involves a newly designed Symmetric key technique "Dehex Algorithm", which encrypts the data with a random key generated and followed by the ECC algorithm. This approach enhances the security of data that is stored in the cloud.
Here, it highlights the importance of securely storing encryption keys using the SHA algorithm, but it addresses the complexity in key management.

Kaur K. (2016) [11] has done research work on "A Double layer encryption algorithm based on DNA and RSA for security on cloud". This paper aims to enhance security by using the combination of DNA and RSA.
However, it encounters the challenges of performance overhead, Key Management Issues, evolving nature of cyber threats.

Thambiraja E, Ramesh G& Umarani, D. R. (2012) [10] have done research work on "A survey on various most common encryption techniques". This paper presents the comparative analysis of existing encryption algorithms and also explains various encryption techniques and their performance.
Here, it presents the security issues, performance parameters because its crucial for selecting right encryption technique, implementation complexity.

Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017, June) [12] have done research work on "Enhanced cloud data security using AES algorithm". This paper aims to enhance the data security in a cloud by using AES encryption for data transfer, and the proposed system denies access of using the user from a third party.

However, it doesn't focus on the data security framework, susceptible attacks towards to data stored, it doesn't thoroughly discuss the implications of the third-party auditor access.

V. CHALLENGES AND BEST PRACTICES OF DOUBLE ENCRYPTION

As the adoption of cloud computing is increasing rapidly, and data breaches become more sophisticated, the need for robust security measures is more critical than ever. Double encryption is a resilient and adaptable solution for the modern digital era. By knowing the complexities involved and implementing informed strategies, it can achieve a balanced approach that maximizes security without compromising performance or operational efficiency.

By adopting best practices, including regular audits, staff training and performance optimization, businesses can mitigate the drawbacks and fully leverage the advantages of double encryption. By carefully considering both the strengths and challenges of this approach, through the analysis of the previous work it can better to prepare ourselves to handle evolving threats of today and tomorrow.

A. Performance Overhead

In Double encryption, the data is encrypted twice, which requires more computational power and time compared to a single encryption technique. By this performance of a system is reduced, highly it effects to the environments with high data throughput or real-time processing needs.

Impact

Processing Time

Double encryption increases the Processing time because the encryption and decryption processes are done twice, which can reduce the performance of applications and services.

More Resource Utilization

Here, resources like CPU, Memory, etc., are required more to handle the double encryption tasks.

Mitigation Strategies

Efficient Algorithms

Choosing efficient algorithms will balance performance and security.

Sufficient Resources

Maintaining adequate resources will handle the encryption task or an increased load.

B. Increased Complexity in Key Management

Maintaining two sets of encryption keys will be a complex task for the key management process, because keys need to be generated securely, rotated, stored, and protected against unauthorized access.

Impact

Key Storage

Securet storage solutions are required for both sets of keys, increasing infrastructure complexity.

Key Rotation and Update

Securing updated and rotated keys of two sets regularly will become complicated.

Risk of Key Loss

Data will be unavailable by losing access to either set of keys.

Mitigation Strategies

Centralized Key Management

Handle the multiple keys by implementing the centralized key management systems.

Automated Key Rotation

Maintaining the key rotation and renewal processes with automated tools.

Robust Backup Systems

Ensure that key backup and recovery systems are in place.

C. *Compatibility and Integration Issues*

Every system, application or cloud service may not be capable of being with double encryption. Existing infrastructure can require custom development to integrate with double encryption.

Impact

Integration costs

It is expensive and time-consuming while integrating and changing the existing system with double encryption.

Operational Disruptions

Shifting the existing system with double encryption will interrupt the existing operations.

Mitigation Strategies

Compatibility Assessments

Before integrating the existing system with double encryption, a compatibility assessment should be performed.

Phased Integration

Moving the existing system with double encryption, disruptions should be minimal.

Vendor Support

The Vendors of the cloud and software should support compatibility.

D. *Higher Costs*

Having the additional resources, a centralized key management system and infrastructure updates will make implementing double encryption expensive.

Impact

Higher Operational Costs and Capital Expenditure

Maintenance, management, additional computational power, hardware and software will lead to an increase in operational costs and capital expenditure.

Mitigation Strategies

Cost-Benefit Analysis

Analysis should be done to determine whether the security with the additional resources will justify the expenses or not.

Budget Allocation

A Specific Budget should be maintained to enhance the security measures.

Efficiency Improvements

Improvements should be done efficiently, which optimizes the existing resources.

E. Potential for Increased Latency

While data accessing and transmission are done with double encryption, latency will occur because of the multiple encryption and decryption processes.

Impact

Application Response and User Experience

Responsiveness of applications, data or resources will be slow because of increased latency, mostly affecting real-time data access.

Mitigation Strategies

Low-Latency Algorithms

For double encryption, choose encryption algorithms that minimize the latency.

Performance Testing

To know latency issues, conduct extensive performance testing.

Edge Computing

Latency will be reduced by collaborating the double encryption with edge computing.

F. Data Recovery and Backup

Data recovery and Backup processes will be a complex task in this double encryption method, because two sets of keys must be available and managed correctly while recovery operations are performed.

Impact

Recovery Time

Data recovery will take more time because the data needs to be decrypted twice.

Risk of Data Loss

While recovering the data, improper management of keys will lead to data loss or corruption.

Mitigation Strategies

Key Backup Solutions

Maintaining proper key backup solutions makes the keys available at the time of recovery.

Identifying Weakness

Regular consistent practices will ensure that the process works efficiently and effectively.

Documentation

Proper documentation should be maintained, which helps in the recovery process and key management.

G. *Risk of Misconfiguration*

Misconfigurations should be avoided by implementing double encryption, which leads to vulnerabilities related to encryption and its keys.

Impact
Vulnerabilities and Operational Issues

Misconfiguration will affect the system functionality and operations, also leading to vulnerabilities, which are exploited by attackers.

Mitigation Strategies
Training and Awareness

Staff should be well-trained so that they can manage and configure the double encryption.

Regular Audits

Misconfiguration can be identified and rectified by performing frequent audits.

H. *Regulatory and Compliance Considerations*

Double encryption meets the regulatory requirements, but it faces additional compliance challenges, such as managing and auditing two sets of encryption keys.

Impact
Compliance Complexity

It is a complex task to maintain compliance with regulations and standards.

Audit Requirements

Detailed audits and documentation are to be maintained by organizations.

Mitigation Strategies
Compliance Frameworks

Align double encryption practices with established compliance frameworks.

Regular Reviews

Frequent reviews are to be conducted to ensure compliance.

Documentation and Reporting

To check audits and compliance, proper documentation and reporting to be maintained.

VI. Case study of Double Encryption in the Banking System

Illustration

How this double encryption secures the customer's data in the digital banking system.

Context

A banking institution handles sensitive information of customers like account numbers, PIN, amount, transaction information, identity proofs, etc. So, it is the responsibility of the bank to secure customer's information in the cloud. To protect the data against unauthorized access, cyberattacks, and threats, the institution is going to adopt double encryption, which boosts the security by protecting data in transmission and at rest.

Implementation
First Encryption Layer

Process

In this First Encryption layer, the customer's data is going to be encrypted with a highly secure symmetric encryption algorithm (Ex, AES–256 in GCM) before sending it to the server.

With the help asymmetric encryption algorithm in the PKI framework, keys are exchanged in an encrypted and authorized format.

Second Encryption Layer

Process

Here, the result of the first encryption layer data is encrypted again by using highly secure symmetric encryption algorithms (Ex, AES, Blowfish, Chacha20) before sending it to the server.

Using an Asymmetric encryption algorithm in the PKI framework, keys are exchanged in an encrypted and authorized format.

Key Management

In double encryption, key management plays a crucial role. This will happen by storing and managing the keys securely with the help of bank's on-premises Hardware Security Modules (HSMs) and Key Management Systems (KMS).

The fully encrypted data is transmitted through the network and reaches to the server, and the encrypted data is stored in cloud storage with identity and access management controls.

Scenario in Action

User Login

A customer logs in to their account by using the bank's mobile application and logs in using 2FA (e.g. Password+OTP). This Session is secured using TLS.

Transaction Request

The customer performs a transaction: sending 3000 to Sravan, Account No: 7321058946.

First Layer Encryption

The complete transaction details (sender information, amount, receiver details) are encrypted by using AES-256-GCM on the client side.

Second Layer Encryption

The result of the first layer of encrypted data is again to be encrypted by using RC6 on the client side itself.

For both layers of encryption, keys are exchanged securely using RSA within the PKI framework.

Finally, the fully encrypted data is sent to a banking cloud server via HTTPS.

Outcome

Performance Overhead

Encrypting the customer's data twice will increase CPU and Memory Usage, mainly on client-side devices.

Mitigation Strategy

Using a light-weight encryption algorithm along with an efficient encryption mode such as AES-GCM.

Increased Complexity in Key Management

Maintaining two distinct key sets will increase complexity for key generation, rotation, and revocation storage.

Mitigation Strategy

So, better to maintain a Centralized key Management system, HSMs for secure storage and automated key life cycle management of banking institutions.

Compatibility and Integration Issues

Some of the cloud services and legacy systems may not support the double encryption mechanism.

Mitigation Strategy

Allowing easy switching or upgrading of encryption algorithms.

Potential for Increased Latency

It delays the processing that will affect the real-time access of the banking application.

Mitigation Strategy

Choosing the stream modes like CTR, GCM, etc.
Performing double encryption for the required data.

Data Recovery and Backup

It is a complex task to maintain data recovery and backup because only authorized keys can perform the data recovery.

Mitigation Strategy

Better to maintain geographically separated HSMs for redundant and secure backups of both keys.

Risk of Misconfiguration

Encryption algorithms and key access controls should be configured correctly otherwise, it leads to vulnerabilities, they will loss customer data.

Mitigation Strategy

To avoid this bank institution has to perform regular audits to identify the weak configuration.

VII. Conclusion

Double encryption enhances cloud data security by adding an extra layer of protection, ensuring confidentiality and compliance. Despite its advantages, double encryption poses challenges such as increased complexity, performance overhead, and higher costs.

It can address the challenges effectively by adopting best practices like efficient key management, regular audits and optimized resource allocation.

In an era of rising cyber threats, double encryption serves as a strategic security measure, enabling businesses to protect their data and maintain resilience in the evolving digital landscape.

References

[1] Nath, M. P., Sridharan, R., Bhargava, A., & Mohammed, T. (2019). Cloud computing: an overview, benefits, issues & research challenges. *idea*, *1*(3). (Services)

[2] Kacha, L., & Zitouni, A. (2018). An overview on data security in cloud computing. *Cybernetics Approaches in Intelligent Systems: Computational Methods in Systems and Software 2017, vol. 1*, 250-261. (security and encryption)

[3] Xue, C. T. S., & Xin, F. T. W. (2016). Benefits and challenges of the adoption of cloud computing in business. *International Journal on Cloud Computing: Services and Architecture*, *6*(6), 01-15.(introduction and services)

[4] Hashemi, S., Monfaredi, K., & Masdari, M. (2013). Using cloud computing for e-government: challenges and benefits. *International Journal of Computer, Information, Systems and Control Engineering*, *7*(9), 596-603. (benefits, services)

[5] Jadeja, Y., & Modi, K. (2012, March). Cloud computing-concepts, architecture and challenges. In *2012 international conference on computing, electronics and electrical technologies (ICCEET)* (pp. 877-880). IEEE. (Services)

[6] Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016, August). Data security in cloud computing. In 2016 Fifth international conference on future generation communication technologies (FGCT) (pp. 55-59). IEEE. (data security and encryption)

[7] Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G. (2021, March). Efficient and secure file transfer in cloud through double encryption using aes and rsa algorithm. In *2021 international conference on emerging smart computing and informatics (ESCI)* (pp. 791-796). IEEE. (aes and RSA weakness and cloud computing definition) thinking.

[8] Rai, D., Desai, R., Tripti, P. S., & Vinutha, B. (2018). Multilevel encryption for cloud storage. *Sahyadri Int J Res*, *4*(1), 40-42.(dE definition)

[9] https://www.kiteworks.com/risk-compliance-glossary/double-encryption-what-it-is-and-why-you-need-it/

[10]Thambiraja, E., Ramesh, G., & Umarani, D. R. (2012). "A survey on various most common encryption techniques". *International journal of advanced research in computer science and software engineering*, *2*(7).(addressing challenges)

[11]Kaur, K. (2016). "A Double layer encryption algorithm based on DNA and RSA for security on cloud". *International Research Journal of Engineering and Technology*, *3*(03), 1742-1745.

[12]Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017, June). "Enhanced cloud data security using AES algorithm". In *2017 International Conference on Intelligent Computing and Control (I2C2)* (pp. 1-5). IEEE.

[13]Soorya Kumar, S., Meenakshi, P., & Subramanyan, (July 2022*) "A. HASHING & DOUBLE ENCRYPTION TECHNIQUE FOR INFORMATION STORAGE IN CLOUD"*. International Journal of Engineering Applied Sciences and Technology, 2022 Vol. 7, Issue 3, Pages 95-99

[14]Akter, R. I. M. A., Khan, M. A. R., Rahman, F. A. R. D. O. W. S. I., Soheli, S. J., & Suha, N. J. (2023). RSA and AES based hybrid encryption technique for enhancing data security in cloud computing. International Journal of Computational and Applied Mathematics & Computer Science, 3, 60-71.

[15]Jana, B., Poray, J., Mandal, T., & Kule, M. (2017, November). “A multilevel encryption technique in cloud security”. In *2017 7th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 220-224). IEEE.

[16]Bharadwaj, Y., & Chakraverty, S. (2013). A design pattern for symmetric encryption. *2013 International Conference on Control, Computing, Communication and Materials (ICCCCM)*, 1-6. https://doi.org/10.1109/ICCCCM.2013.6648912.

[17]Alenezi, M., Alabdulrazzaq, H., & Mohammad, N. (2020). Symmetric Encryption Algorithms: Review and Evaluation Study. *Int. J. Commun. Networks Inf. Secur.*, 12. https://doi.org/10.54039/IJCNIS.V12I2.4698.

[18]Ragavan, K., B, M., Vivekrabinson, K., & Arun, R. (2024). A Double Layer Encryption for Communication using Cryptographic Algorithms. *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, 1-7. https://doi.org/10.1109/ic-ETITE58242.2024.10493432.

[19]Abdullah, D., Rahim, R., Siahaan, A., Ulva, A., Fitri, Z., Malahayati, M., & Harun, H. (2018). Super-Encryption Cryptography with IDEA and WAKE Algorithm. *Journal of Physics: Conference Series*, 1019. https://doi.org/10.1088/1742-6596/1019/1/012039.

[20]Abhiram, L., Gowrav, L., Kumar, H., Sriroop, B., & Lakkannavar, M. (2014). Design and synthesis of dual key based AES encryption. *International Conference on Circuits, Communication, Control and Computing*, 85-88. https://doi.org/10.1109/CIMCA.2014.7057763.

[21]Shao, Z., Tang, Y., Liang, M., Shang, Y., Wang, F., & Wang, Y. (2020). Double image encryption based on symmetry of 2D-DFT and equal modulus decomposition. *Multimedia Tools and Applications*, 80, 8973 - 8998. https://doi.org/10.1007/s11042-020-09961-9.

[22]Hasija, T., Ramkumar, K., Singh, B., Kaur, A., & Mittal, S. (2023). Symmetric Key Cryptography: Review, Algorithmic Insights, and Challenges in the Era of Quantum Computers. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1-6. https://doi.org/10.1109/ICCCNT56998.2023.10307081.

[23]P.G, S., & Rajesh, S. (2018). Double Encryption using TEA and DNA. *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, 1-5. https://doi.org/10.1109/ICCSDET.2018.8821117.

[24]Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security algorithms for cloud computing. *Procedia Computer Science*, *85*, 535-542.

[25]Malhotra, A., Arora, A., & Bhatia, M. (2022). Symmetric Cryptographic Approaches. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2022.47982.

[26]Ma, L., Qu, M., & He, P. (2023). Double encryption algorithm for massive personal biometric authentication images based on chaotic mapping for future smart cities. *Journal of Testing and Evaluation*, *51*(3), 1447-1460.

[27]Zhang, Y., Yu, C., Wang, Y., Han, J., Zhong, M., An, H., & Yuan, N. (2023, June). Application of Symmetric Key Algorithm in Data Security Design of Smart Grid. In *2023 International Conference on Mechatronics, IoT and Industrial Informatics (ICMIII)* (pp. 143-147). IEEE.

[28]Chatterjee, D., Nath, J., Das, S., Agarwal, S., & Nath, A. (2011). Symmetric key Cryptography using modified DJSSA symmetric key algorithm. In *Proceedings of the*

International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[29]https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing

M. Pravallika – M. Pravallika received an M.Sc degree in Computer Science from Dr.Abdul Haq Urdu University, Kurnool. Currently, she is doing a Ph.D. in Computer Science at Sri Padmavati Mahila Visvavidyalam (Women's University), Tirupati, Andhra Pradesh, India. Her research interest lies in the area of Cloud Computing and Cyber Security.

Dr. P. Bhargavi - Dr. P. Bhargavi is an Assistant Professor in the Department of Computer Science at Sri Padmavati Mahila Visvavidyalayam (Women's University), Tirupati, Andhra Pradesh, India. She has 27 years of teaching experience and 17 years of research experience. Nine Ph.Ds were awarded and Five Ph.D. scholars are being guided under her supervision. More than 70 papers published in reputed journals. Presented 35 papers in international and National conferences. Eleven book chapters are published and authored three books. She has Published 3 patents and one Patent granted in her credit. She has conducted three International and one National conference, many hands-on workshops & faculty development programs and acted as Session Chair of International and national conferences. Completed two minor project from DST-CURIE-AI, SPMVV, Tirupati.

She is appointed as Director,Computer Center, Assistant Coordinator of CURIE-AI Center, member in Placement cell, Coordinator for University E-office. She is member in IEEE, CSI, ISTE, ACM, IAENG and, MEACSE. Her research interest is in Artificial Intelligence, Machine Learning, Soft Computing, Big Data Analytics, Cloud Computing, Bioinformatics and GIS. She acted as Editorial Board Member of International Journal of IJCAR, Technical Committee Member of IndiaCOM2016 and Reviewer of IndiaCOM2016 and IGI book chapter.